

Contact:**Hervais Simo Fhom**

06151/ 86960041

hervais.simo@sit.fraunhofer.de

Prof. Dr. Claudia EckertInstitutsleitung Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt

Telefon +49 (0) 61 51/8 69-399

Telefax +49 (0) 61 51/8 69-224

Bachelor Thesis

TOPIC: Design and Implementation of Privacy Enhancements in Browser-based Identity Federation Models**Background:**

Browser-based Identity federation is the means by which Web sites and applications offers Internet users cross-domain single sign-on, which lets them authenticate once and thereafter gain access to protected resources and Web sites hosted in other security domains. In this way, browsing the web and accessing online services becomes easier and requires less effort. Another advantage is the reduction of deployment costs since the service provider outsources users authentication to a third party named identity provider. Despite such benefits, Identity federation models entail new privacy risks due to the fact that user's privacy sensitive identity attributes (e.g. name, age, gender, etc.) are transferred from identity provider to the service provider with an intermediate step at the browser. For instance, current versions of SAML, the only open standard nowadays and OpenID the today's most prominent web-based federated identity model introduce privacy threat where a malicious identity provider could track user's activities. Moreover, both models offer privacy features such as the selective attribute disclosure or the proof of conditions on identity attributes only to a limited extend. To overcome this shortcoming, we have advocated privacy extensions which enable the identity provider to confirm that conditions over attributes hold, rather than having to reveal their exact values. Such extensions would leverages advanced Anonymous Credential schemes to support selective disclosure of user identity attributes and proof of conditions on such attributes.

Tasks:

- Identification and analysis of relevant use cases that motivate the need for trust and privacy enhancement in current Web-based Identity federation models;
- Analysis of the state-of-the art, possible attacker motivations and shortcomings of the relevant identity federation models. OpenID and SAML are to be considered as references;
- With regard to the analysis results, proposal for an Anonymous Credentials-based authentication protocol either within the OpenID or the SAML framework;
- Prototypical implementation of the proposed protocol using Idemix an Anonymous Credential system developed at IBM Research Lab.

Required Skills:

- Knowledge in IT security as well as Java programming skills
- Knowledge of OpenID, SAML specifications and privacy-enhancing technologies as well

Date of entry: Immediately